Dirk Fox

Seitenkanalangriffe

Hintergrund

Angriffe auf IT-Systeme sind besonders erfolgversprechend, wenn sie auf eine Art und Weise erfolgen, die die Designer und Entwickler des Systems in ihrer Konzeption nicht berücksichtigt haben. Ein Weg, solche übersehenen Angriffsflächen eines Systems zu entdecken, ist die Suche nach nicht offensichtlichen Kanälen, „Nebenzugängen", die Informationen über das System preisgeben oder einen direkten Zugriff ermöglichen. Da bei der Entwicklung eines Systems nur selten alle impliziten Sicherheitsannahmen explizit gemacht werden, werden solche „Seitenkanäle" (*side channel*) häufig übersehen: ein Update-Mechanismus, der das Einspielen manipulierten Codes erlaubt; ein „Debugging-Mode", der Informationen über den Inhalt von Registern preisgibt; oder ein Fehlerzustand, in den man das System versetzen kann, um Daten bspw. aus dem Speicher auszulesen.

Seitenkanalangriffe auf eingebettete Systeme

Angriffe über Seitenkanäle sind ein besonders viel versprechender Weg, um Schutzmechanismen eingebetteter Systeme zu überwinden. Da der Datenaustausch (z. B. das Protokoll einer Chipkarte mit einem Lesegerät oder eines Fahrzeugschlüssels mit der Bordelektronik) bei einem gut geschützten System verschlüsselt erfolgt, ist das Hauptziel eines Angreifers der Verschlüsselungsschlüssel.

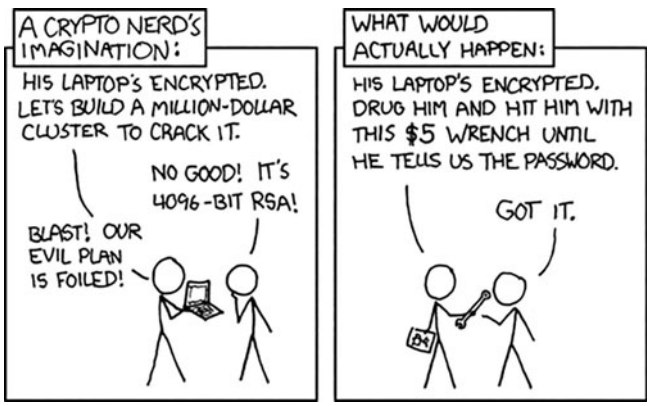
Auch wenn dieser gut geschützt in einer unzugänglichen Hardware gespeichert ist, können Seitenkanäle Informationen über den Schlüssel preisgeben, die dessen Rekonstruktion erlauben. Zu diesen Seitenkanälen zählen insbesondere die folgenden, die in den vergangenen Jahren ausgenutzt werden konnten (siehe auch [1, 2, 3]):

- **Abstrahlung**: Jedes IT-System erzeugt während der Durchführung von elektronischen Operationen Magnetfelder. Diese elektromagnetische Abstrahlung kann z. T. sogar aus größerer Entfernung noch gemessen werden und so Rückschlüsse auf die Operationen und die dabei verwendeten Daten erlauben.
- **Stromverbrauch**: Je nach Kryptoverfahren kann der Stromverbrauch des Devices in Abhängigkeit von den Schlüsselbits variieren – z. B. wenn das Verfahren bei einer „0" eine Operation mit geringerem Verbrauch durchführt als bei einer „1". Der Verbrauch (und seine Schwankung) kann bei einem eingebetteten System meist ohne zerstörenden Eingriff gemessen werden.
- **Zeitbedarf**: Auch die Rechenzeit eines Kryptoverfahrens kann variieren, je nach dem, welche Operationen bei einem „0"- und bei einem „1"-Bit des Schlüssels ausgeführt werden. Aus dem Zeitbedarf für die Verschlüsselung kann dabei möglicherweise der Schlüssel rekonstruiert werden.
- **Speicherbedarf**: Schließlich kann der Speicherbedarf für die Ablage von Zwischen- oder Teilergebnissen einer kryptographischen Berechnung Rückschlüsse auf Schlüsselbits erlauben.

Gegenmaßnahmen

Alle diese Angriffe sind mit teilweise erheblichem Aufwand verbunden, denn sie müssen auf die verwendeten Algorithmen und das eingebettete System zugeschnitten werden. Umgekehrt sind Gegenmaßnahmen häufig einfach. So lassen sich z. B. mit zusätzlichen, wirkungslosen Operationen Zeitverhalten und Stromverbrauch „glätten", und die Abstrahlung des Systems kann durch Schirmung verhindert werden.

Abb. 1 | Seitenkanalangriffe in der Praxis (Quelle: Randall Munroe, http://xkcd.com/)



Referenzen

[1] Petra Wohlmacher, Dirk Fox: *Hardwaresicherheit von Smartcards*. DuD 5/1997, S. 260-265.

[2] Stefan Mangard, *Die physikalische Sicherheit eingebetteter Systeme*, DuD 12/2012, S. 867-871.

[3] Hermann Drexler, Lars Hoffmann: *Krypto-Angriffe über Seitenkanäle*. (In diesem Heft.)